

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号  
特開2003-167805  
(P2003-167805A)

(43)公開日 平成15年6月13日(2003.6.13)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テマコード <sup>*</sup> (参考)
G 0 6 F 13/00	3 5 3	G 0 6 F 13/00	3 5 3 C 5 B 0 8 9
H 0 4 L 12/46	2 0 0	H 0 4 L 12/46	2 0 0 X 5 K 0 3 3

審査請求 有 請求項の数7 O L (全 10 頁)

(21)出願番号 特願2001-370464(P2001-370464)  
(22)出願日 平成13年12月4日(2001.12.4)

(71)出願人 000004226  
日本電信電話株式会社  
東京都千代田区大手町二丁目3番1号  
(72)発明者 吉良 雄介  
東京都千代田区大手町二丁目3番1号 日  
本電信電話株式会社内  
(72)発明者 小野 諭  
東京都千代田区大手町二丁目3番1号 日  
本電信電話株式会社内  
(74)代理人 100077274  
弁理士 磯村 雅俊 (外1名)

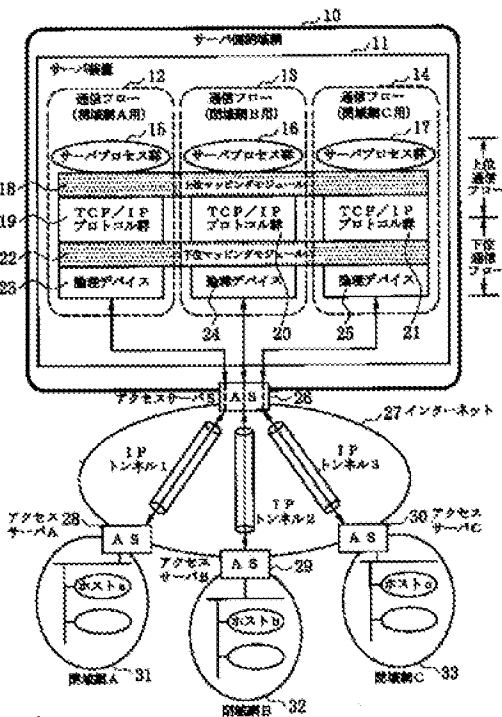
最終頁に続く

(54)【発明の名称】 複数ユーザ側閉域網とサーバ側閉域網間のネットワーク通信方法およびサーバ装置

(57)【要約】

【課題】サーバ側閉域網の物理的に1台のサーバ装置を、各ユーザ側閉域網間で共有せず、各ユーザ側閉域網に独立して提供することで、専用サーバとしての動作をさせる。

【解決手段】複数ユーザ側閉域網31〜33は、サーバ側閉域網10とIPトンネルを用いてアクセスサーバ26、28〜30により接続を行う。接続要求があると、アクセスサーバ26はどの閉域網の要求かを識別し、ユーザ側閉域網に固有の識別符号をパケットタグ付けし、サーバ装置11に転送する。サーバ装置11は、プロトコルスタック19〜21までの上位通信フローと、プロトコルスタック19〜21から論理デバイスインタフェース23〜25までの下位通信フローを複数備え、これらの通信フロー12〜14をユーザ側閉域網31〜33に割り当てる。サーバ装置11は、受信したパケットの識別タグから送信元ホストの閉域網を特定する。



## 【特許請求の範囲】

【請求項1】 複数のユーザ側閉域網と1Pトンネルを用いてアクセスサーバにより接続を行うサーバ側閉域網内に物理的に1台のサーバ装置を用いた網間ネットワーク通信方法であって、

サーバプロセス群とプロトコルスタックとの組み合わせを記憶し、かつ前記サーバプロセス群とプロトコルスタックとのリンクを記憶した内容に従って制御するモジュールにより管理される上位通信フローと、物理ネットワークインタフェースまたは論理デバイスインタフェースと前記プロトコルスタックとの組み合わせを記憶し、かつ前記プロトコルスタックを該当する物理ネットワークインタフェースまたは論理デバイスインタフェースにリンクさせるモジュールにより管理される下位通信フローとの組み合わせからなる通信フローを複数用意し、前記通信フローをユーザ側閉域網ごとに1つずつ割り当てることにより、各ユーザ側閉域網と前記サーバ装置間における前記サーバ装置内の個々の通信経路をネットワーク上、論理的に分離することを特徴とする複数ユーザ側閉域網とサーバ側閉域網間のネットワーク通信方法。

【請求項2】 請求項1に記載のネットワーク通信方法において、前記通信フローごとの物理ネットワークインタフェースまたは論理デバイスインタフェースにネットワークを介して接続する各ユーザ側閉域網との通信では、当該通信フローのプロトコルスタックとサーバプロセス群とを用いて各ユーザ側閉域網に独立したサーバサービスの提供を行うことを特徴とする複数ユーザ側閉域網とサーバ側閉域網間のネットワーク通信方法。

【請求項3】 請求項1または2に記載のネットワーク通信方法において、前記複数の通信フローごとの物理ネットワークインタフェースまたは論理デバイスインタフェースに対し、1Pアドレスの重複した割り当てを許容することを特徴とする複数ユーザ側閉域網とサーバ側閉域網間のネットワーク通信方法。

【請求項4】 複数のユーザ側閉域網と1Pトンネルを用いてアクセスサーバにより接続を行うサーバ側閉域網に設けられる物理的に1台のサーバ装置であって、サーバプロセス群とプロトコルスタックとの組み合わせを記憶し、かつ前記サーバプロセス群とプロトコルスタックとのリンクを記憶された内容に従って制御することにより、上位通信フローを管理する手段と、物理ネットワークインタフェースまたは論理デバイスインタフェースと前記プロトコルスタックとの組み合わせを記憶し、かつ前記プロトコルスタックを該当する物理ネットワークインタフェースまたは論理デバイスインタフェースにリンクさせることにより、下位通信フローを管理する手段と、上位通信フローと下位通信フローとの組み合わせからな

る通信フローを複数装備し、前記通信フローをユーザ側閉域網ごとに1つずつ割り当てることにより、各ユーザ側閉域網と前記サーバ装置間における前記サーバ装置内の個々の通信経路をネットワーク上、論理的に分離する通信手段とを具備することを特徴とするサーバ装置。

【請求項5】 請求項4に記載のサーバ装置において、前記通信フローごとの物理ネットワークインタフェースまたは論理デバイスインタフェースにネットワークを介して接続を行う各ユーザ側閉域網との通信では、当該通信フローのプロトコルスタックとサーバプロセス群とを用いて、各ユーザ側閉域網に独立したサーバサービスを行う仮想サーバ提供手段を具備することを特徴とするサーバ装置。

【請求項6】 請求項4または5のいずれかに記載のサーバ装置の動作をコンピュータに実現させるためのサーバ装置用プログラム。

【請求項7】 請求項6に記載のサーバ装置用プログラムを格納したことを特徴とするコンピュータ読み取り可能な記録媒体。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、インターネットやプライベートネットワークを介して接続された複数の異なる閉域網間での通信を行うエクストラネット向けのアプリケーションホスティングサービスや情報共有サーバサービスなどのネットワーク通信方法およびその装置に関し、例えば物理的に1台のサーバを用いて複数のユーザ側閉域網にアプリケーションを提供するサーバサービスや、サーバを介してファイルやデータベースなどを複数のユーザ側閉域網に共有化するサービスを行うための複数ユーザ側閉域網とサーバ側閉域網間のネットワーク通信方法およびサーバ装置に関する。

## 【0002】

【従来の技術】インターネットを始めとするネットワーク通信の利用は広く普及しており、企業やコミュニティなどは通信コストを安く抑えつつ安全な通信を行うために閉域網を利用してイントラネットやエクストラネットを構築している。また、近年、閉域網は大企業のみならず中小企業やSOHO（Small Office Home Office）でも用いられており、その数は増加の傾向にある。さらに、閉域網を用いてLAN（Local Area Network）内LAN（例えば、イントラネットの中にさらに階層的なネットを構築した形態）を構築する等、閉域網の利用形態も多様化している。

【0003】このような小規模多数化している閉域網にサーバサービスを提供する方法として各閉域網にサーバを設置する方法があるが、コストや稼働がかかりサーバを設置する側の負担が大きい。そこで、物理的に1台のサーバを用いて各閉域網にサーバサービスを行うのでは

あるが、インターネット通信機能とサーバプロセスとを各ユーザ側閉域網間で共有することなく、各々のユーザ側閉域網に独立した提供を可能にして、各閉域網にそれぞれ専用サーバがあるかのような動作を可能にする仮想プライベートサーバの構築を考えることにする。

【0004】閉域網の構築には、グローバルアドレスの取得に手間とコストがかかるために、ローカルアドレスを用いる方法が多く採用されている。このように構築されている複数の閉域網に対して、物理的に1台のサーバを用いてサーバサービス提供を考えた場合、次のような問題の解決が必要となる。

- (1) サーバ側閉域網を含めた閉域網間でのローカルアドレス空間の衝突
- (2) サーバを介して他の閉域網をまたぐ等の不正アクセス
- (3) サーバから各閉域網内にあるホストへの接続の確立
- (4) サーバ側を含む閉域網の追加や網構成変更の容易性

【0005】複数のユーザ側閉域網とサーバ側閉域網との間で通信を行うための従来技術としては、L2TP (Layer 2 Tunneling Protocol) やIPsec (IP security protocol) などに代表されるIP (Internet Protocol) トンネル技術、NAT (Network Address Translation) やR-NAT (特開2001-016255号公報参照: Root side-Network Address Translation) に代表されるアドレス変換技術、さらにIPトンネル技術とアドレス変換技術の両者を用いる技術の3つがある。

【0006】なお、IPトンネル技術の一つであるIPsecのトンネルモードは、閉域網内からのIPパケットに広域ネットワーク内での転送に使用するIPヘッダを付与してカプセル化し、かつ暗号化処理を施すことにより、閉域網間をセキュアに接続する仮想トンネルを作成する技術である。L2TPでは、端末から公衆電話網を経由して、インターネットプロバイダなどに設置されたアクセスサーバに接続し、さらにこのサーバから閉域網内に用意されたサーバと仮想的なトンネルを確立することにより、端末と閉域網内との間でPPP (Point-to-Point Protocol) による接続を確立したようなみせるものである。また、NATは、LANをインターネットに接続する際に、LAN側で使用されているプライベートIPアドレスをインターネット側で割り当てられているグローバルIPアドレスに変換する方法を規定したものである。

【0007】今、ここにユーザ側閉域網A、Bがインターネットを介してサーバ側閉域網SにIPトンネルを用いて互いの網間アクセスサーバにより接続されているも

のとする。ユーザ側閉域網A、Bに属する各ホストとSに属するサーバは、それぞれアドレス空間A、B、Sが割り当てられている。この構成により、各ホストは同じ閉域網に属するサーバと接続しているように見せることができる。これにより、各閉域網に割り当てられているローカルアドレスをそのまま使用することが可能になる。しかし、閉域網では、ホストにローカルアドレスを自由に割り当てるので、ユーザ側閉域網間やユーザ側閉域網とサーバ側閉域網間でアドレス空間が重複する場合がある。ユーザ側閉域網間でアドレス空間が重複する場合、サーバから見ると同一のアドレスを持つホストが複数存在していることになり、サーバはどのホストと通信しているのかを正しく認識することができない、という問題が生じる。

【0008】また、ユーザ側閉域網に属し、ローカルアドレスを割り当てられたホストがインターネット上のグローバルアドレスを割り当てられたサーバと通信を行うためには、そのホストもグローバルアドレスを持つ必要がある。この時、閉域網とインターネットとの境界に設けたNAT装置にグローバルアドレスを静的に割り当て、このグローバルアドレスとホストに割り当てられたローカルアドレスとを対応付けることにより、ホストとサーバ間の接続を可能にする。

【0009】しかし、NAT技術は、ローカルアドレスを割り当てられたホストからの接続要求によってそのローカルアドレスとグローバルアドレスとを動的に対応付けて接続の識別を行うために、ホストからの接続要求によって確立されるホストとサーバ間の接続が一旦切断されると、その接続に用いたローカルアドレスとグローバルアドレスとの対応は効力を失ってしまうので、グローバルアドレスを割り当てられたサーバからローカルアドレスを静的に割り当てられたホストへの情報発信などブッシュ型サービスは不可能となる。さらに、サーバは閉域網の識別を行うことができないため、各閉域網に属するホストに対して閉域網に固有のサービスや情報を提供することが困難になる、という問題が生じる。

【0010】そこで、複数のユーザ側閉域網とサーバ側閉域網とをそれぞれのIPトンネルを用いて接続し、IPトンネルを終端するサーバ側閉域網のアクセスサーバにおいて、ユーザ側閉域網のホストとIPトンネルのペアに対して固有となるIPアドレスを割り当て、これを記憶する。このIPアドレスとホストに割り当てられたローカルアドレスとを対応付けることにより、ホストとサーバ間の接続を可能にする。このように、閉域網を特定するアドレス空間の中からホストごとに異なるIPアドレスを用いてアドレスの変換を行うため、接続してくるユーザ側閉域網間でのローカルアドレス空間の衝突回避やサーバから特定ホストへの接続を可能にしている。

【0011】しかし、それぞれのユーザ側閉域網では、サーバが自分らの網内に属しているかのように自由なロ

ーカルアドレスを用いてサーバにアドレスを割り当てることは許されない。他のユーザ側閉域網に使用されているローカルアドレス空間や他のユーザ側閉域網がサーバへの割り当てを希望しているローカルアドレス空間を考慮した上で、各ユーザ側閉域網に固有のサーバアドレスを決定しなくてはならないという問題が生じる。その結果として、物理的に1台のサーバを用いて各ユーザ側閉域網にそれぞれ専用サーバがあるかのように動作させるという環境が満たされていない。

【0012】さらに、ある1つのサーバアプリケーションを各ユーザ側閉域網に提供する際に、サーバは共通のサーバプロセスを用いて全てのユーザ側閉域網に提供を行っていることが多く、サーバ内部におけるユーザ側閉域網間の分離はサーバに接続してくるアドレスの違いによってのみ行われるため、サーバを介して他のユーザ側閉域網をまたぐ等の不正アクセスの防止ができなくなるとともに、サーバおよびサーバ上で実行されるサーバアプリケーションが常にアドレスの違いを意識したカスタマイズを強要されるので、設定する箇所が多くなり、その結果、閉域網の追加や網構成の変更が困難になる、という問題が生じる。

#### 【0013】

【発明が解決しようとする課題】従来、インターネット通信においては、TCP/IPプロトコル群がホストやルータなどの機器の間での通信に使用されている。そのTCP/IPプロトコル群はインターネットプロトコルスタックと呼ばれる。このプロトコルスタックの役割として、サーバ装置の物理ネットワークインタフェースまたは複数の仮想的な論理デバイスインタフェースに割り当てられるIPアドレス（サーバアドレス）の保持、パケット配送のための経路（ルーティング）情報の保持、各プロトコルパケットの処理などインターネット環境でのネットワーク通信機能を担う。

【0014】図2は、従来のインターネットプロトコルスタックを示す図である。物理層およびデータリンク層を含むリンク層63は、ハードウェアインタフェース（ドライバを含む）632、ARP（Address Resolution Protocol）633、およびRARP（Reverse Address Resolution Protocol）631によって構成される。ARP633は、IPアドレスからそのIPアドレスに対応するノードのハードウェアアドレス（MACアドレス等）を要求するためのプロトコルであり、RARP631は、これとは逆に、自ノードのMACアドレスを元に、自ノードのIPアドレスを要求するためのプロトコルである。

【0015】ネットワーク層62は、IP処理部622、ICMP（Internet Control Message Protocol）623、およびIGMP（Internet Group Managem

ent Protocol）621によって構成される。ICMP623は、IPプロトコルの状態に関する情報を管理するために使用されるプロトコルであり、IGMP621はIPマルチキャストを実現するためのプロトコルである。

【0016】トランスポート層61は、TCP（Transmission Control Protocol）612とUDP（User Datagram Protocol）611によって構成される。TCP612は、IPの上位プロトコルで、コネクション型で信頼性の高い通信を提供し、UDP611はコネクションレス型のプロトコルで、信頼性確保のための処理を実施しないため、TCPに比べ高速に処理できる。アプリケーション層60は、ユーザプロセス601によって、エンドユーザでユーザが直接利用する通信サービスを提供する。

【0017】従来のサーバ装置には、プロトコルスタックが1つのみ用意されており、このサーバ装置と通信を行うホストやルータは、このプロトコルスタックによって提供されるインターネット通信機能とこのプロトコルスタックを通して提供されるサーバプロセスとを共有して利用している。従って、複数のユーザ側ネットワークに対してサーバサービスを展開するサーバ装置の場合、その多くがユーザ側ネットワークごとに区別してサービスを行わなければならないために、サーバ装置において、ユーザ側ネットワークの特定と分離が必要である。

【0018】従来のサーバ技術では、サーバに向けて送信されるパケットの送信元アドレスや送信先アドレスの違いを利用してユーザ側ネットワークの特定と分離を行うが、ユーザ側ネットワークがローカルアドレス空間を自由に割り当てることができる閉域網により構築されている場合には、閉域網間におけるローカルアドレス空間の衝突を回避するために、アドレスの制限や変換など強制的なアドレス管理を行い、閉域網間の特定と分離を行い易くしている。しかし、サーバ装置のネットワーク通信機能とサーバプロセスとをユーザ側ネットワークの各々に共有して提供することは、アドレス管理等により、閉域網の特徴である閉域性、サーバからの自発的な情報配信であるプッシュ型サービス、閉域網の追加や網構成変更の容易性などのネットワークサービスの実現を難しくしている。

【0019】そこで、本発明の目的は、これら従来の課題を解決し、複数のユーザ側閉域網がサーバ側閉域網とIPTunnelを用いてアクセスサーバにより接続を行うネットワーク通信において、サーバ側閉域網に設置する物理的に1台のサーバ装置により提供されるインターネット通信機能とサーバプロセスとを各ユーザ側閉域網間で共有することなく、各々のユーザ側閉域網に独立した提供を可能にし、そのサーバ装置が各々のユーザ側閉域

網に属している専用サーバであるかのような動作を実現することができる複数ユーザ側閉域網とサーバ側閉域網間のネットワーク通信方法およびサーバ装置を提供することにある。

#### 【0020】

【課題を解決するための手段】上記目的を達成するため、本発明による複数ユーザ側閉域網とサーバ側閉域網間のネットワーク通信方法では、サーバ装置において、サーバプロセス群からプロトコルスタックまでの上位通信フローと、プロトコルスタックから物理ネットワークインタフェースまたは論理デバイスインタフェースまでの下位通信フローとの組み合わせからなる通信フローを複数装備し、この通信フローをユーザ側閉域網ごとに1つずつ割り当てることにより、各ユーザ側閉域網とサーバ間のサーバ内における個々の通信経路をネットワーク上、論理的に分離し、複数接続しているユーザ側閉域網の特定と分離を実現する。

【0021】本発明のサーバ装置は、各ユーザ側閉域網に割り当てた固有の通信フローを用いて、プロトコルスタックが担うサーバアドレスの保持、パケット配送経路の制御、各プロトコルパケットの処理などのインターネット通信機能とWebサーバ、FTPサーバなどのサーバプロセスとを独立して提供し、ユーザ側閉域網間は他のユーザ側閉域網と通信フローを共有されることなく、ネットワーク上、論理的に閉域性を保持したままサーバ装置との通信を実現する。

【0022】本発明により、複数のユーザ側閉域網がサーバ側閉域網とIPトンネルを用いてアクセスサーバにより接続を行うネットワーク通信において、サーバ側閉域網に設置する物理的に1台のサーバ装置によって提供されるインターネット通信機能とサーバプロセスとを各ユーザ側閉域網間で共有することなく、そのサーバ装置が各々のユーザ側閉域網に属している専用サーバであるかのように動作することが可能になる。

#### 【0023】

【発明の実施の形態】以下、本発明の実施例を、図面により詳細に説明する。図1は、本発明のネットワーク間通信方法を実現するシステム概念図である。

（構成）ここでは、通信フローおよび外部接続が3の場合の構成を示している。複数のユーザ側閉域網（A）31、（B）32、（C）33がサーバ側閉域網10との間で、IPトンネルを用いてアクセスサーバ26、28、29、30により接続を行っている。各ユーザ側閉域網31～33に属するホストa、b、cは、サーバ側閉域網10に設置する物理的に1台のサーバ装置11からサーバサービスの提供を受ける。なお、サーバ側閉域網10のアクセスサーバ装置26のホスティングサービスについては、特開2001-016255号公報に記載の『閉域網間接続システムと閉域網間接続方法およびその処理プログラムを記録した記録媒体ならびにホス

ティングサービスシステム』を参照されたい。

【0024】サーバ装置11は、通信フローを200程度（図中では3個、12、13、14）備えており、各々のプロトコルスタック19、20、21は図2に示すように、従来のインターネットプロトコルスタックと同じである。すなわち、サーバプロセス群15、16、17とTCP/IPプロトコル群19、20、21とが上位マッピングモジュール18を介して接続され、これらTCP/IPプロトコル群19、20、21と論理デバイスインタフェース23、24、25とが下位マッピングモジュール22を介して接続されている。サーバ装置11は、論理デバイスインタフェース23、24、25をこれらのプロトコルスタックと同数だけ備えている。

【0025】サーバ装置11は論理デバイスインタフェース23、24、25のそれぞれにリンクするプロトコルスタック19、20、21と各プロトコルスタック19、20、21にリンクするサーバプロセス群15、16、17とを組み合わせることができる通信フロー12、13、14により、ユーザ側閉域網31、32、33間をネットワーク上、論理的に分離し、各々のユーザ側閉域網31、32、33に独立したサーバサービスの提供を行う。以下では、各ユーザ側閉域網31、32、33のホストa、b、cがサーバ側閉域網10に設置されるサーバ装置11を利用するための実施例について説明する。

【0026】図3は、本発明における閉域網の識別にVLANタグを用いた場合のネットワーク間通信方法の動作説明図である。

（通信準備）それぞれの閉域網31、32、33では、ローカルアドレスを自由に用いて各ホストa、b、cに割り当てており、他の閉域網の存在を知らないものとする。ホストaは、閉域網31に属しており、IPアドレスLa（192.168.1.10）が割り当てられている。ホストbは閉域網32に属しており、IPアドレスLb（192.168.1.10）が割り当てられている。また、ホストcは閉域網33に属しており、IPアドレスLc（192.168.1.10）が割り当てられている。閉域網31、32、33間では、ローカルアドレス空間が衝突する可能性があるため、本実施例では故意に衝突させている。

【0027】サーバ側閉域網10のアクセスサーバ（S）26と各ユーザ側閉域網31、32、33のアクセスサーバ（A）28、（B）29、（C）30には、グローバルIPアドレスとして、それぞれGs（129.60.1.1）、Ga（129.60.2.1）、Gb（129.60.3.1）、Gc（129.60.4.1）が割り当てられている。

【0028】ユーザ側閉域網31はサーバ装置11にローカルアドレスSa（192.168.1.1）を、ユーザ側閉域網32はSb（192.168.1.1）を、ユーザ側閉域網33はSc（192.168.1.1）を割り当てようとしている。各ユーザ側閉域網31～33がサーバアドレスにローカルアドレ

ス空間を自由に割り当てる場合、閉域網間でサーバアドレスが衝突する可能性があるため、本実施例においては故意に衝突をさせている。この要求に従い、サーバ装置11側では、閉域網31用として割り当てる通信フロー12の論理デバイスインタフェース23 (dev0) に対してサーバアドレスS a (192.168.1.1)を、閉域網32用として割り当てる通信フロー13の論理デバイスインタフェース24 (dev1) に対してサーバアドレスS b (192.168.1.1)を、閉域網33用として割り当てる通信フロー14の論理デバイスインタフェース25 (dev2) に対してサーバアドレスS c (192.168.1.1)を、それぞれ割り当てる。

【0029】このとき、図3に示す下位マッピングモジュール22では、論理デバイスインタフェース23、24、25とプロトコルスタック19、20、21との間の下位通信フローを管理し、プロトコルスタック19、20、21を該当する論理デバイスインタフェース23、24、25にリンクさせると同時に、それぞれ下位通信フローを構成するプロトコルスタック19、20、21と論理デバイスインタフェース23、24、25とのペア、およびこの下位通信フローを利用する閉域網の代わりとなるVLAN (Virtual LAN) タグ34、35、36をセット [(inet0, dev0) ⇔ vlan600]、[(inet1, dev1) ⇔ vlan601]、[(inet2, dev2) ⇔ vlan602]にして、テーブルに記憶する。つまり、VLANタグ34、35、36の値が閉域網を識別する。従来のサーバ装置では、インターネットプロトコルスタックを1つしか持たないため、複数の論理デバイスインタフェースに対して同じサーバアドレスを割り当てることはできなかったが、本発明においては、プロトコルスタックを複数装備することにより、これを可能にしている。

【0030】次に、各ユーザ側閉域網31、32、33がサーバ装置11をWebサーバとして利用することを考える。サーバ装置11は、サーバプロセス15、16、17がどの閉域網によって利用されるかをプロセスのグループIDにより認識する。ユーザ側閉域網31にはグループID (gid1000)、ユーザ側閉域網32にはグループID (gid1001)、ユーザ側閉域網33にはグループID (gid1002)を割り当て、各閉域網31、32、33が利用するWebサーバのサーバプロセスはそれぞれに割り当てられるグループIDを以って実行される。このとき、図3に示す上位マッピングモジュール18では、サーバプロセス群15、16、17とプロトコルスタック19、20、21との間の上位通信フローを管理し、サーバプロセス15、16、17を該当するプロトコルスタック19、20、21にリンクさせると同時に、それぞれの上位通信フローのプロトコルスタックとグループIDとのペア [(inet0 ⇔ gid1000)、(inet1 ⇔ gid1001)、(inet2 ⇔ gid1002)]をテーブルに記憶する。

【0031】以上で、上位通信フローと下位通信フローとの組み合わせによってできる通信フロー12、13、14の準備が各ユーザ側閉域網31、32、33に対して完了する。以下では、各ユーザ側閉域網31、32、33のホストa、b、cがサーバ側閉域網10に設置されるサーバ装置11と通信を行う方法について説明する。

#### 【0032】(通信動作)

(ユーザ側閉域網のホストからサーバ装置へ) ユーザ側閉域網31、32、33に属する各ホストa、b、cがWebサーバとしてのサーバ装置11と通信することを考える。まず、ホストaは、閉域網31内に構築したローカルなDNS (Domain Name System) によりサーバ側閉域網10に属するサーバ装置11のローカルアドレスS aを取得する。そして、アクセスサーバ(A)28に向けてパケットを送信する。他のホストb、cも、同様にそれぞれアクセスサーバ(B)29、(C)30に向けてパケットを送信する。

【0033】ホストaからパケットを受け取ったアクセスサーバ(A)28は、IPトンネリング処理を行う。すなわち、ホストaのIPアドレスL aとサーバアドレスS aを含むIPパケットヘッダをアクセスサーバ(A)28、(S)26のグローバルアドレスでカプセル化し、インターネットを経由してアクセスサーバ(S)26にパケットを送信する。他のアクセスサーバ(B)29、(C)30においても、同様の処理が行われ、それぞれがアクセスサーバ(S)26にトンネリングされたパケットを送信する。

【0034】アクセスサーバ(A)28からパケットを受け取ったアクセスサーバ(S)26は、カプセルを解くと、ここから先の通信においてパケットの送信元である閉域網31を特定可能にするため、IPトンネルとVLANタグのペア [(Ga,Gs) ⇔ vlan600]をテーブルに記憶しており、該当するタグ(vlan600)をパケットに付与する。そして、脱カプセル後のIPヘッダに従い、サーバ装置11に向けてパケットを送信する。このとき、閉域網32に属するホストb、閉域網33に属するホストcからの通信も全く同様である。それぞれのIPトンネルとVLANタグのペア [(Gb,Gs) ⇔ vlan601]、[(Gc,Gs) ⇔ vlan602]を記憶したテーブルに従って、それぞれVLANタグ(vlan601)と(vlan602)がパケットに付与される。

【0035】アクセスサーバ(S)26からタグ付きパケットを受け取ったサーバ装置11では、そのVLANタグ(vlan600)にマッチするプロトコルスタック19と論理デバイスインタフェース23のペア (inet0, dev0)を下位マッピングモジュール22のテーブルより選択し、該当する通信フロー12へパケットを転送する。その通信フロー12の中で、パケットは論理デバイスインタフェース (dev0) 23からプロトコルスタック (In

10

20

30

40

50

et0) 19までの下位通信フローを経由し、同プロトコルスタック19にリンクされているWebサーバのサーバプロセス (gid1000) 15へ上位通信フローを使って届けられる。このとき、ホストb、ホストcからの通信も、全く同様のプロセスにより処理される。

【0036】以上、サーバ装置11にとって、La、Lb、Lcのように送信元のIPアドレスが衝突しても、また各々のユーザ側閉域網31、32、33が割り当てたサーバアドレスがSa、Sb、Scのように衝突しても、サーバ装置11内部において通信フロー12、13、14をネットワーク上、論理的に分離しており、サーバサービスを各閉域網31、32、33と全く独立して提供することができる。

#### 【0037】(通信動作)

(サーバ装置からユーザ側閉域網のホストへ) 次に、Webサーバがホストaに返答パケットを送信することを考える。Webサーバのサーバプロセス (gid1000) 15は、自らがリンクしているプロトコルスタック (inet0) 19に対して上位通信フローを使ってパケットを返す。同プロトコルスタック19の各プロトコルにおいてパケット処理が行われた後、下位通信フローを管理する下位マッピングモジュール22のテーブル [(inet0, dev0) ⇔ vlan600] に従って、パケットにはVLAN (vlan600) がタグ付けされ、下位通信フローの論理デバイスインタフェース (dev0) 23からアクセスサーバ(S) 26に向けてパケットを送信する。このとき、ホストb、cに対する返答パケットも、全く同様のプロセスにより処理される。

【0038】サーバ装置11からタグ付きパケットを受け取ったアクセスサーバ(S) 26は、IPTunnelとVLANタグのペア [(Ga,Gs) ⇔ vlan600] を記憶したテーブルに従って、IPTunnelリング処理を行う。すなわち、サーバアドレスSaとホストaのIPアドレスLaとを含むIPパケットヘッダをアクセスサーバ(S) 26、(A) 28のグローバルアドレスでカプセル化し、インターネットを経由してアクセスサーバ(A) 28にパケットを送信する。このとき、ホストb、cに対する返答パケットも全く同様であり、IPTunnelとVLANタグのペア [(Gb,Gs) ⇔ vlan601]、[(Gc,Gs) ⇔ vlan602] に従って、アクセスサーバ(B) 29、(C) 30にそれぞれパケットを送信する。

【0039】アクセスサーバ(S) 26からパケットを受け取ったアクセスサーバ(A) 28は、カプセルを解くと、脱カプセル後のIPヘッダに従い、ホストaに向けてパケットを送信する。最終的にホストaがパケットを受け取る。同様に、ホストbはアクセスサーバ(B) 29から、ホストcはアクセスサーバ(C) 30からパケットを受け取る。

【0040】(新たなユーザ側閉域網に対するサービス展開) 既に登録されているユーザ側閉域網(A) 31、

(B) 32、(C) 33に対して、新たにユーザ側閉域網(D) が追加登録された場合、サーバ側閉域網10では下記のように対処する。未使用の通信フローの中から1つを選び、

(1) プロトコルスタック: (inet3)

(2) グループID: (gid1003)

(3) 上位マッピングモジュール: [(inet3⇔gid1003)]

(4) 下位マッピングモジュール: [(inet3,dev3)⇔vlan603]

(5) アクセスサーバ(S): [(Gd,Gs)⇔vlan603] を施すことにより、他の閉域網の環境を変更することなく、容易に新たなユーザ側閉域網(D) に対して仮想サーバサービスを展開することができる。

【0041】(サーバ装置) 図4は、本発明の一実施例を示すサーバ装置の構成図である。図4に示すように、本発明のサーバ装置11は、複数のプロセスを処理するサーバプロセス41と、サーバプロセス群からプロトコルスタック多重構成部46までの上位通信フローを管理する上位マッピングモジュール42と、プロトコルスタック多重構成部46から物理ネットワークデバイス多重構成部51までの下位通信フローを管理する下位マッピングモジュール47とから構成される。上位マッピングモジュール42と下位マッピングモジュール47は、いずれも組み合わせ記憶部44、49と、これに結合されたリンク制御部43、45および48、50から成る。

【0042】サーバ装置11は、サーバプロセス41からプロトコルスタック46までの上位通信フローと、プロトコルスタック46から物理ネットワークインタフェースまたは論理デバイスインタフェース51までの下位通信フローとの組み合わせからなる通信フローを複数整備する。これらの通信フローをユーザ側閉域網ごとに1つずつ割り当てることにより、各ユーザ側閉域網とサーバ装置間のサーバ内における個々の通信経路をネットワーク上で論理的に分離し、複数接続しているユーザ側閉域網の特定と分離を実現している。

【0043】サーバ装置11は、各ユーザ側閉域網に割り当てた固有の通信フローを用いて、プロトコルスタック多重構成部46が担うサーバアドレスの保持、パケット配送経路の制御、各プロトコルパケットの処理などのインターネット通信機能と、Webサーバ、FTP (File Transfer Protocol) サーバなどのサーバプロセスとを独立して提供し、ユーザ側閉域網間は他のユーザ側閉域網と通信フローを共有することなく、ネットワーク上、論理的に閉域性を保持したまま、サーバ装置11との通信を行うことが可能である。

【0044】このように、物理的には1台のサーバ装置11であるが、サーバプロセス41がリンク制御部45により制御されることにより、複数のサーバプロセス群となり、さらにリンク制御部43の制御により、プロト

コルスタック多重構成部46が複数のプロトコルスタックを構成する。上位マッピングモジュール42は、サーバプロセス群とプロトコルスタックとの組み合わせを記憶するとともに、サーバプロセスを該当するプロトコルスタックにリンク制御することにより、上位通信フローを管理する。また、下位マッピングモジュール47は、物理ネットワークインタフェースまたは論理デバイスインタフェースの多重構成部51とプロトコルスタック46との組み合わせを記憶するとともに、プロトコルスタックを該当する物理ネットワークインタフェースまたは

10 論理デバイスインタフェースにリンク制御することにより、下位通信フローを管理する。さらに、上位通信フローと下位通信フローとの組み合わせからなる通信フローを複数整備し、これらの通信フローをユーザ側閉域網ごとに1つずつ割り当てることにより、各ユーザ側閉域網とサーバ装置間の個々の通信経路をネットワーク上、論理的に分離する。

【0045】(サーバ装置用プログラム) 図4および図5の動作番号「0041」～「0044」で説明したサーバ装置の動作をプログラムに変換し、変換したプログラムをCD-ROMなどの記録媒体に記録しておけば、サーバ側閉域網の任意のサーバ装置のコンピュータにこの記録媒体を装着し、プログラムをインストールして実行させることにより、本発明を容易に実現することができる。

#### 【0046】

【発明の効果】以上説明したように、本発明によれば、複数のユーザ側閉域網がサーバ側閉域網とIPトンネルを用いてアクセスサーバにより接続を行うネットワーク通信において、サーバ装置により提供されるサーバ機能とサーバプロセスと各ユーザ側閉域網間で共有することなく、各々のユーザ側閉域網に独立して提供することができる。その結果、サーバ側閉域網に設置する物理的に1台のサーバ装置が各々のユーザ側閉域網に属している専用サーバであるかのように動作させることが可能になる。その結果、今後増加すると予想される複数企業間でのデータ交換を必要とするプロジェクトの実施時や調達業務の実施時に必要となる複数閉域網向けの共用サーバの構築、運用などを提供するハウジングサービスへの展

開が可能となる。

【0047】また、このサービスは、自社の閉域網に手を加えることなく、複数の他企業と情報の連携が可能になるため、ISPなどが行っているVPNサービスの新しい付加サービスとしての展開が見込める。さらに、企業のみならず、個人向けのポータルサイトサービスへの展開も可能になる。また、本発明では、1つのサーバ装置に対して、各ユーザ側閉域網の管理者は、自由にアドレスを付与することができ、プッシュプル型サービスを受けることができる。このように、本発明は、閉域網向けの新しい情報流通プラットフォームを構築する手段としての利用を見込める、という顕著な効果を奏する。

#### 【図面の簡単な説明】

【図1】本発明のネットワーク間通信方法を適用するネットワーク構成図である。

【図2】従来のインターネットプロトコルスタックを示す図である。

【図3】本発明の一実施例を示すネットワーク間通信方法の動作説明図である。

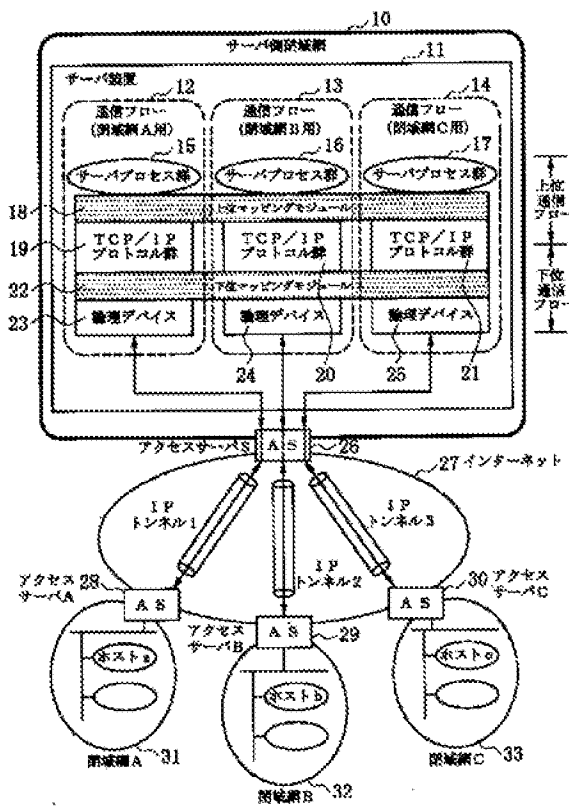
【図4】本発明の一実施例を示すサーバ装置の構成図である。

#### 【符号の説明】

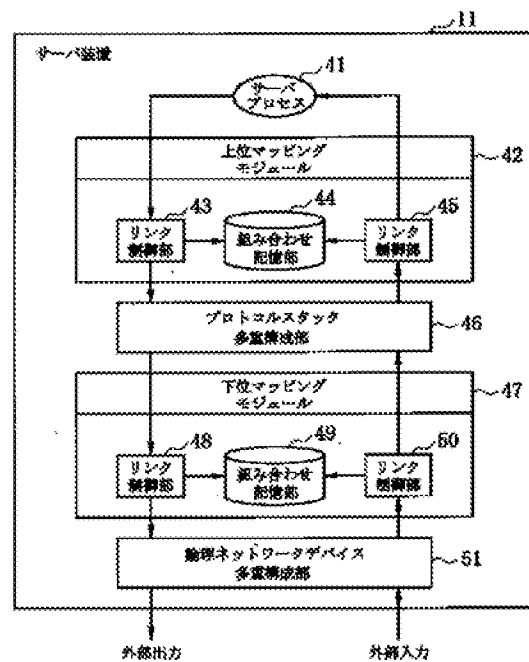
10…サーバ側閉域網、11…サーバ装置、12…通信フロー(閉域網A用)、13…通信フロー(閉域網B用)、14…通信フロー(閉域網C用)、15、16、17…サーバプロセス群、18…上位マッピングモジュール、19、20、21…TCP/IPプロトコル群、22…下位マッピングモジュール、23、24、25…論理デバイスインタフェース、26…アクセスサーバ(S)、27…インターネット、28、29、30…アクセスサーバ(A)、(B)、(C)、a、b、c…ホスト、31、32、33…閉域網(A)、(B)、(C)、34、35、36…VLANタグ、41…サーバプロセス、42…上位マッピングモジュール、43、45…リンク制御部、44…組み合わせ記憶部、46…プロトコルスタック多重構成部、47…下位マッピングモジュール、48、50…リンク制御部、49…組み合わせ記憶部、51…論理ネットワークデバイス多重構成部。



【図1】



【図4】



【図2】

